Winter 12-10-2002

# A Model Architecture to Combat Security Issues in Mobile Commerce

Raj Gururajan

Chaiyaporn Chirathamjaree

# A Model Architecture to Combat Security Issues in Mobile Commerce

Raj Gururajan
School of Information Technology
Murdoch University
South Street, Murdoch, 6150, Australia
r.gururajan@murdoch.edu.au

Chaiyaporn Chirathamjaree
School of Computer & Information Science
Edith Cowan University
2 Bradford Street, Mt. Lawley, 6050, Australia
c.chirathamjaree@cowan.edu.au

## Abstract

The security of transactions in mobile commerce is moving away from being just an IT concern to being a business concern because of the potential loss of revenue to businesses due to lack of privacy, integrity or confidentiality, system slowdown or downtime. While most security procedures are limited to corporate IT infrastructure, in mobile commerce, issues concerned with transaction security appear to have extended beyond the corporate network to embrace the complete business process. Any lapse in procedures that maintain the confidentiality of data or the violation of privacy could affect corporate image and hence would impact on customer relationships. In turn, any adverse effect on customer relationships would impact negatively on business revenue. In addition to existing security problems in a wired commerce environment, the emergence of mobile devices has renewed calls for addressing security threats to financial transactions. These problems are discussed in this paper as key issues in terms of an organization's architectural and procedural approaches to the security, reliability and availability of business transactions.

**Keywords:** Mobile commerce, security threats, IT security, risks, business transactions.

## 1. Introduction

In the past, the majority of the computer security officers have had difficulty in convincing management to allocate financial resources for IT security. However, with the emergence of electronic commerce and various legislations, organizations appear to have understood the necessity for computer security, especially data security [5]. The current trend in most organizations, therefore, appears to be one of security officers focussing on IT security – namely – hardware security, software security and access security [5]. Access security involves both physical access and logical access. What appears to be missing from these security procedures is the proper integration of business transactions. Ghosh [11] states that while various security measures have dealt independently with business transactions, electronic commerce and the emerging mobile commerce have changed the perception that an independent IT infrastructure security alone can protect an organization in terms of its business needs. To support Ghosh's statement, Deise et. al. [7] has identified the shift in the focus of IT security in organizations, resulting in new security policies to focus on reliable, available and trusted business transactions.

Initially in this paper, the new security threats arising from mobile commerce are highlighted. These threats are then linked to financial transactions in order to highlight the potential loss or damage to an organization's revenue. The organizational IT requirements are assessed with a view to providing support for financial transactions in a mobile commerce environment. This organizational support is then formed into an 'architecture' and the architecture is discussed in terms of how it supports an organization and what it does to support financial transactions in particular. This architecture is subsequently elaborated in terms of a series of action items so that transaction security in an organization can be guaranteed. It is hoped that these action items would then enable organizations to tighten their current security strategies.

## 2. Security Threats Arising from Mobile Commerce

Security threats in mobile commerce can range from the passive eavesdropping of messages to actively stealing data [19]. In a radio frequency operated mobile commerce environment, it is possible to listen to conversations with minimum difficulty. This has an impact on consumers causing concern about their data and about voice messages from unauthorized access. At the other end of the problem is the inherent security risk involved in transferring information over networks. This problem consists of two components: *identification integrity*, and *message integrity*. Identification integrity refers to the signature elements found in the messages which establish where the

message originates. Message integrity refers to details to establish that the message is received as sent and that no third party has attempted to open, modify or alter the contents. According to Zhang & Lee [25], these two items appear to cause a lot of concern to both senders and receivers. While the senders risk the theft or misuse of their personnel information such as account and bank details, the receivers (usually a merchant) risk repudiation of the transactions and the resultant non-payment.

Further security concerns in mobile commerce arise from the development in the technology itself [25]. It is envisaged that mobile technology will be offered with payment for the range of services offered. This is already emerging in the domain of mobile telephones. For instance, when a mobile telephone user accesses other network carriers, a special charge is levied on the user. Therefore, it is safe to assume that there will not be any "free services" in the future. The technology is developing in such a way that the payment for such services will be through some form of "smart card". The details stored in the smart card will need to be transmitted via the networks for validation and verification in order to determine service levels. If these networks are not fully secure, security breaches may occur.

One major security breach that can happen in mobile commerce is when user details are transformed from one mobile network to another [13]. When this transformation occurs, any encrypted data needs to be decrypted for transparency. In mobile commerce, when mobile devices make requests to the web pages of a network server, a four-stage process is followed. First, the requests arise from the originating Wireless Transport Security Layer (WTSL) protocol. Second, the requests are translated at the originating Wireless Application Protocol (WAP) gateway. Third, they are sent to the standard Session Security Layer (SSL) protocol of the destination network. Fourth, the translated information reaches the Hyper Text Transfer Protocol (HTTP) modules in the new network in order for the requests to be processed. In the course of translating one protocol to another, the data is decrypted and then re-encrypted. This process is commonly known as the "WAP Gap". If an attacker is able to have access to the mobile network at this point, then simply capturing the data when it is decrypted can compromise the security of the session.

Data in the Mobile Commerce environment is secured using encryption technology. According to Ghosh [11], it has already been proven that this technology is vulnerable to attack. Hackers have broken some of the existing algorithms for encryption, so there is nothing like complete security. Further, there is no international regulatory framework available to enforce certain security related problems. For example, in the current climate, no individual organization or government can guarantee security to consumers. When a security breach appears in an international transaction, no one country will be able to assume responsibility to prosecute the perpetrators. While these problems have been recognised and solutions are being proposed, organizations are losing consumer confidence. This has the potential to impact the revenue generated by these organizations.

Trust is central to any commercial transaction and more so in the case of mobile commerce [9]. Trust is normally generated through relationships between transacting parties, familiarity with procedures, or the redress of mechanisms. In the case of mobile commerce, the need for creating the trust in the consumer assumes extreme importance because of its virtual nature. It hinges on assuring consumers and businesses that their use of network services is secure and reliable, that their transactions are safe, that they will be able to verify important information about transactions and transacting parties such as origin, receipt and integrity of information, as well as the identification of parties dealt with. Therefore. the challenge is not to make mobile commerce foolproof, but to make the system reliable enough so that the value greatly exceeds the risk.

Any new development in technology in today's consumer mind creates both curiosity and reluctance. The informality and lack of overall of control creates the perception that the Internet is inherently insecure [20]. This perception can trigger business and technological risks [21]. Business risks involve products and services, inadequate legal provisions, the reliability of trading partners, the behaviour of staff and the possible demise of the Internet service provider. Technological risks involve hacker attacks, computer viruses and data interception. To achieve satisfactory levels of trust, organisations have to think about managing both business and technological risks. Currently mobile commerce relies mostly on knowledge-based trust that is useful for Business-to-Business commerce [9]. However, there is a big surge in identification-based trust to satisfy consumers' concerns about their transaction details. In addition, the current architecture for mobile communications does not provide full security in terms of transaction integrity. Some of the models envisaged for mobile commerce are based on a smart card approach and hence the issue of financial transaction security needs greater examination.

## 3. Security Threats that Can Impact Financial Transactions

Security risks in a mobile commerce environment associated with financial transactions can be categorised into traditional risks and non-traditional risks [14]. Traditional risks usually involve loss or damage to tangible physical assets and resulting economic loss. For example, loss of computer hardware may have an impact on incomplete transactions. Alternatively, a missing data disk, which is not fully protected from theft can place an organisation at risk. Treatment of traditional risks is usually addressed in risk management policies. Protecting tangible assets from traditional perils, even when those assets are devoted to mobile commerce, does not involve new and different techniques. These security treats are beyond the scope of this paper.

Non-traditional risks involve damage to organisations'

computer systems and electronic data [24]. These risks include stolen information, damage to web sites by hackers, the hijacking of web sites and viruses. An attack may be perpetrated for any number of reasons including financial gain involving credit card fraud, curiosity with no specific intent of harm, espionage by domestic or foreign competitors, or foreign governments, revenge by a terminated employee who is intent on wiping out files, disclosure of personal data to unauthorised institutions as in health related cases, thrill seeking, disruption to stop critical activities, and extortion for financial or political reasons. Any attack, internal or external, on a computer system is disruptive and forces the administrator to shut down the system resulting in revenue loss.

Non-traditional security breaches also include unauthorized access or the use of a company's computer system and data by an outsider or an insider [7]. For example, a hacker could break into a company's computer system and steal or destroy data. Widespread use of mobile commerce enhances the possibility of an outsider invading an organisation's computer system. Due to the reliance on computers for daily operations, breaches of a company's computer or information security system are a risk to almost all functional components of the business. Use of software to encrypt and, thus, safeguard communications provides some protection, but also adds the risk that a virus or other bug could damage the equipment or data. Further, according to Dang [6], theft of information such as critical electronic files including financial data, customer information, marketing and new product data, trade secrets, and personnel data may provide competitors with a strategic advantage, criminals with the means to commit fraud, and others the opportunity to disparage the company. Moreover, Dornan [8] states that the use of misappropriated information may harm third parties such as customers, employees, and business partners. The theft of information may undermine an acquisition or cause a public relations problem and hence potential loss of revenue.

Security breaches may be very costly to an organisation [10]. When an unauthorized access to the computer is gained for the purposes of committing a crime such as fraud, reputation is also at stake. Other security issues include the prohibition of high-level encryption technology by domestic or foreign governments so that agencies can break the codes if necessary for defence or law enforcement, changes in international standards, and loss of encryption key recovery.

## 4. A Closer Look at Fraud and Crime Risks in Mobile Commerce

The scope of computer fraud and crime is immense in mobile commerce. Among the most common crimes are malicious mischief, such as the insertion of viruses or Trojan horses into one or more computer systems; the fraudulent transfer of money to personal accounts; the use of forged electronic signatures; the theft of credit card information and credit card fraud; Medicare and Medicaid fraud; the theft of intellectual property; illegal use of software; stock and commodity market manipulations; and similar illegal activities. Most losses are insurable, but premiums will be relatively exorbitant if security measures are not appropriately enacted [13].

A hacker may use a number of methods such as the insertion of viruses, spamming and web snatching to access computer systems and data and to cause damage. Damage may occur at data centers or in the transmission networks, routers, or power sources. Virus attacks may also come from innocent parties who pass on an infection without knowledge that the system is contaminated, usually by e-mail.

By using another technique, *distributed denial of service*, hackers have been able to attack some of the most well-known and highly secure web sites in the world, including Yahoo.com, eBay.com, and amazon.com. This technique hijacks numerous computers on the Internet and instructs each one to flood a target site with phoney data. The target site, trying to accommodate the phoney data, becomes overworked and soon begins to lose memory. The result is effectively slowing or shutting down the entire site to real customers.

*Web snatching* is a practice in which one party plants a virus in another party's Web site that automatically moves the viewer from the selected site to a site run by the web snatcher. This is done without the permission of the selected Web site owner or the site visitor. In many instances, the viewer is unable to get out of the unwanted site, short of turning off the computer, so is effectively held hostage to the new site. The diverted-from and diverted-to sites usually have nothing in common with each other.

Financial institutions and companies that have inadequate electronic security protection are more likely than not to suffer losses of money, information, or other corporate assets. Surveys have shown that most companies and institutions have incurred losses, and a substantial number have no idea whether they have come under electronic attack or not. Insiders or former insiders have committed most of the electronic crime and fraud, but there are many examples of third-party fraud and theft.

Mobile commerce can only be conducted if all parties believe there is adequate security. The majority of those who use the Internet, on which current mobile commerce technologies are built, are very concerned about security [11]. Some 40 percent of Internet consumers give false information when they use the Web because they do not trust the Internet's security [4]. Other users refuse to register at sites that require what the consumer believes to be personal information [1]. Many people want the government to legislate security on the Internet as they are not confident that businesses will do the job on their own [23]. Therefore, it is critical that businesses enhance both their security and their security image to combat crime on the Internet, as well as to increase customer confidence and participation in virtual business environments.

## 5. Security Risks in Mobile Commerce

## Emerging from Reliance on Third Parties

Today, most organisations rely on computers for their daily operations. Traditional and non-traditional security risks can interrupt a business or literally shut it down. For example, a security breach by a hacker can severely disrupt a business and those who depend on it. Most businesses in mobile commerce are dependent in several ways on the continued reliability and operation of computer controlled systems not within their control, such as the telephone network which is managed and controlled by computers. Businesses are dependent on their financial institutions that are also managed and controlled by computers. In mobile commerce, to accommodate home users, organisations are dependent on their Internet Service Providers (ISP). Suppliers and customers depend on each other's electronic data systems and on mutual systems, such as a third-party commodity exchange. When one system fails, it may cause the other systems to fail as well. Failure may be a slowdown in the dependent system, also called the 'brownout' or a total denial of service, also called the 'blackout' [11]

The above risks can result in many different types of losses [2] [8] [22]. Traditionally, property losses have meant damage to a building or other business property, including computer equipment. In the mobile commerce world, however, the focus is on damage to computer networks and, more importantly, to data. An important issue is whether data is considered tangible property under a typical property insurance policy. It appears that insurers are only beginning to address the issue of what is defined as 'covered property' under their policies at it is more likely that, in the long run, the courts will have to decide on this issue.

Property losses can also occur when an organisation's intangible or intellectual property is infringed or violated. Copyrighted materials can be copied without permission, trademarks can be infringed upon or diluted, and patented property or ideas can be stolen. Today, a firm's intellectual property may be its most valuable asset [7]. In mobile commerce, organisations need to be extra vigilant in protecting their intellectual property from hackers, crackers, competitors, and others, as well as make sure they do not infringe the intellectual property rights of third parties. This could potentially expose a firm to third-party liability.

Time losses typically include business interruption (BI) losses and service interruption losses. A BI loss is the economic loss resulting from the interruption of business activities. Business interruption losses may result from the inability to access data, the theft of data, or a threat to the integrity of a database. For example, a breach in the security of a credit card database may cause the database owner to curtail activity on the system until a damage assessment is completed and the system integrity is re-established. Not only is there a disruption of the database operations, there is also a consequential effect on all third-party users of the system.

Service interruption losses include economic losses associated with the interruption of utilities. A service interruption incident can occur from an "off-site" exposure or event. There have been many incidents of communication cables inadvertently being cut. Long-distance telecommunication companies have experienced software problems in data routing that effectively crippled their networks for several days. According to Lee [17], service denials may cause a customer business interruption, network suspension, or a disruption in or delay of services. Service denials may result in damage claims or lawsuits for breach of a service contract.

Mobile commerce gives rise to new implications for doing business and being protected from interruptions [3]. Businesses suffering losses related to server outages face the risk of losing customers for extended periods of time. In mobile commerce, the increased reliance on suppliers is also exposing businesses to new risks for financial losses. These range from suppliers of goods (such as raw materials) to suppliers of services (such as server usage, delivery services, electricity, and telephones).

Business interruption may have several consequences - e.g., loss of income; extra expenses to recover; loss of customer, partner, and shareholder confidence; and, ultimately, reduced market capitalization. In some cases, business interruption may constitute a breach of contract and third parties harmed by the denial of service may sue, adding liability losses to first-party damages.

## 6. Expense Incurred by Organizations due to Business Interruptions

In the event of an interruption, a business may incur extraordinary expense to resume operations as quickly as possible. An example of extra expense might be increased freight charges to avoid delays in the production process associated with a loss event. In the mobile commerce area, there are new types of costs in the context of risk and insurance, including the costs of operating a web site from an alternative server, the costs of operating a web site through an alternative provider, the costs of repairing web sites damaged by hackers or equipment failures, and the costs of rebuilding other lost information [18]. Thus, various security risks arising from a combination of issues warrant closer scrutiny of the assessment of an organisation's IT requirements in order to facilitate secure financial transactions.

## 7. Assessment of Organization's IT Requirements

In order to guarantee the security of transactions in mobile commerce, the initial assessment of an organisation's IT requirement is essential for a number of reasons [16]. These include ever-changing customer requirements, changing hardware and software platforms, changing user needs and user experiences gained from innovative IT products. Therefore, such an assessment involves the four key components of mobile commerce.

They are (1) embedded computers in many everyday objects [12]; (2) next generation wireless networks [10]; (3) interfacing technologies for bi-directional communications [5]; and (4) design of an application that satisfies user needs [6].

The first key component, embedded computers, arises from the projected increase in wireless devices by 2005 and the prediction that, by 2005, mobile devices will outnumber wired devices [15]. These mobile devices would consist of some form of embedded system and hence the allocation of priority. The next component, wireless networks, follows from the first one which highlights the need for networks to be wireless (to support the concept of mobility and hence mobile devices). Users communicate via a number of different mobile devices and hence bi-directional communication is essential for an organisation to ensure that transactions are reliable and secure. Finally, the fourth component, application design, needs to accommodate diversity of user demands.

When an organisation's IT requirements are being assessed, importance should also be given to 'user experiences'. In the mobile commerce environment, user experiences typically involve cameras, music and other innovative technologies such as positioning systems and hence organisations should find a way to accommodate these ever changing user experiences. Organisations would then be tempted to add additional hardware and software resources to their existing infrastructure to accommodate these innovative technologies but this would increase their financial burden. One emerging suggestion appears to be the consideration of 'interface' facilities to enable the sharing of other third-party resources. This requires address and connectivity mechanisms that do not exist today. While recent newspaper articles forecast that such capabilities are emerging, the challenge for organisations is to create applications that truly have this multi-modal, multi-channel character because it is believed that the immediacy of wireless technology is great.

With this in mind, if we analyse an organisation's IT infrastructure, then we would be able to sort business needs to support secure transactions into four main groups. They are:

1. Technical infrastructure that can identify what IT consists of in an organisation;
2. Physical components of IT that can identify how these components support various workflow requirements in an organisation;
3. Logical components that can identify how IT components support various business processes; and
4. Real time measurement and control of security and service levels in real time.

While the first three points provide essential components of an application architecture in an organisation, the fourth provides the control and maintenance components of the application architecture. Real time control is essential in mobile commerce because of the difficulty in describing complete security architecture to ensure security of transactions.

## 8. The Architecture

The architecture, shown in Figure 1, consists of 10 levels, starting from level 0. The level 0 is where all security policies that ensure transaction security are dealt with. This is a management component and independent of the organisation's IT infrastructure. This is because in the mobile commerce environment, due to changing user needs, it is difficult for the security officer alone to ensure the reliability of transactions. It is essential that management assumes the overall responsibility with security officers providing the necessary infrastructure because it is the managers who know the various processes involved in conducting financial transactions. This view is quite different from the current electronic commerce environment where security officers are responsible for data and information security. While this may be possible in a wired environment, due to importance given to the information and its origin in a mobile commerce environment, the view is totally different. Organisations will need to align their business processes with proper security policies because it will be difficult to track users in a mobile commerce environment due to the possibility of 'roaming'.

Further, in mobile commerce environment, users, systems and transactions change rapidly and unpredictably. This requires organisations to accommodate these needs and yet provide reliable and secure transactions. The current static authentication and authorisation process will be superseded in mobile commerce and the new dynamic privilege management will be an essential component. Therefore, risk management associated with an organisation's IT security will also need to be dynamic and to operate in real time to react to incidents and threats more pro-actively. In essence, level 0 of the architecture will ensure that customers, business partners, and other stakeholders of a transaction such as banks and governments interact directly with these business applications and their IT environments, especially in mobile environments. Level 0 architecture will ensure that the transaction environment is up and running, reliable and secure.

The levels 1-3 put the customer first and are specific to business needs. At these levels, several independent business activities are integrated through IT applications to ensure that the data, functions and workflow modules of an organisation are synchronised. Due to increasing demand from customers for mobile commerce, visibility and interaction across the supply chain to the customer are essential. Therefore, manual sub-transactions, usually found in a traditional transaction model (including weaker electronic commerce models), need to disappear and levels

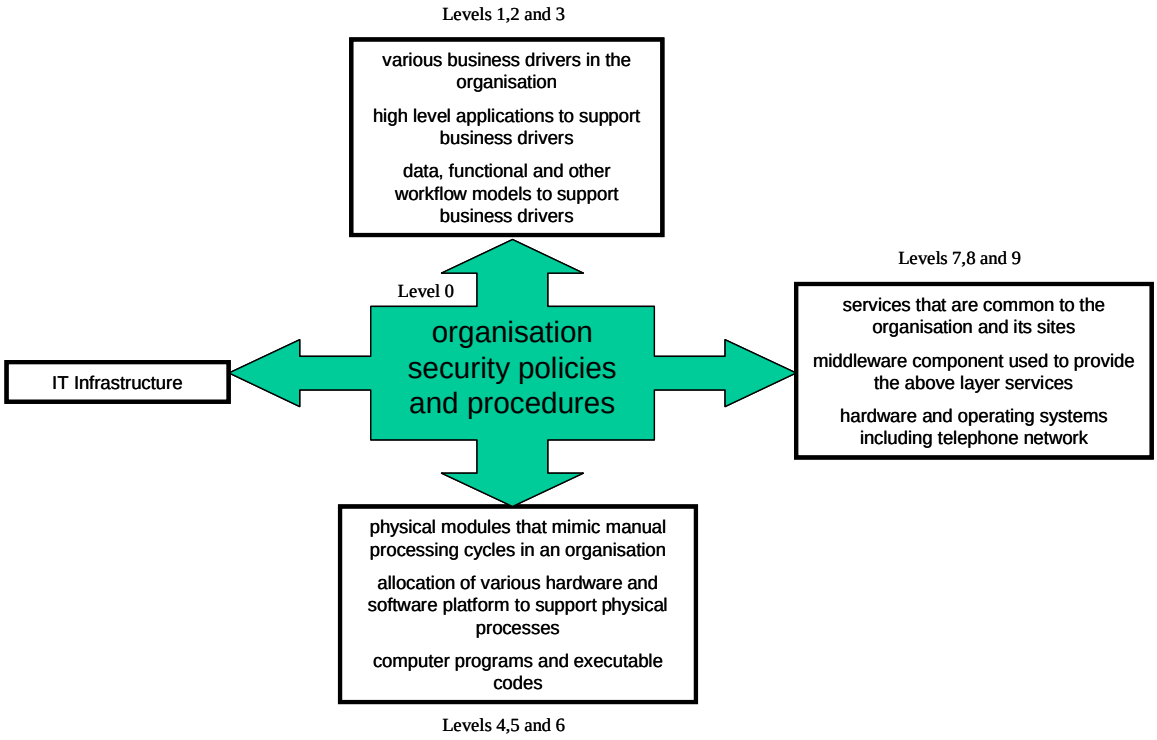


**Figure 1 The Architecture**

1-3 will ensure that this happens. Levels 4-6 consist of the various physical modules to support the workflow. These levels also consist of the 'code' needed to support workflow and the integration of workflow. These levels are of extreme importance to businesses because these are where the integration of multiple segments of a business such as CRM and SCM takes place. Further, due to the physical nature of IT components, this is where the existing resources are integrated with new resources. To establish financial security, levels 4-6 need to be maintained properly because the transaction is split into multiple components at these levels before it is processed. Further, when the transaction is split into component sub-transactions, each of the sub-transaction may run on varied systems with different infrastructures. Organisations, therefore, should focus their 'security' on these levels for successful mobile-commerce. The last three levels are comprised of IT components in order to realise the various combinations of business needs. At these levels, IT components such as a computer are added to the existing infrastructure. While the previous levels 4-6 facilitate business needs, levels 7-9 actually implement them. Issues such as network speed and transaction completion time are essential characteristics at these levels. While the business performance is measured at the previous levels, response time measurement is controlled in the last three levels (7-9). These three levels are vulnerable to attack and the implementation of security procedures starts at these levels.

## 9. Discussion

When a financial transaction is facilitated in a mobile commerce environment, the consumer usually accesses the organisation's computer to search for appropriate details. Once the consumer is satisfied with his/her order, an order is placed. The consumer places an order using the infrastructure provided by the Internet storefront and using his or her payment method of choice. Once the order reaches the organisation, the transaction is processed. A number of security issues, such as, verifying the credentials of the consumer arise at this point. Provision for real-time security and connectivity to authorise payment via the Internet or wireless medium forms an integral component of the transaction. The organisation channels the transaction through various financial networks such as banks, ensuring that customers are authorized to make their purchase.

When security issues are applied to a transaction, the client/server architecture for transaction processing is usually used. The client is installed on the organisation's merchant site by the third-party providing user authentication for financial details and this client is integrated with mobile commerce application. The client is usually pre-integrated with store management systems including those for management reporting purposes.

For the purposes of transaction authorization, the client software establishes a secure link with the processing server over the Internet using an SSL connection, and transmits the encrypted transaction request. The server, which is a multi-threaded processing environment, receives the request and transmits it over a private network to the appropriate financial processing network.

Depending upon the consumer's financial status, the transaction is approved or denied. When the authorization response is received from the financial network, the response is returned via the same session to the client on

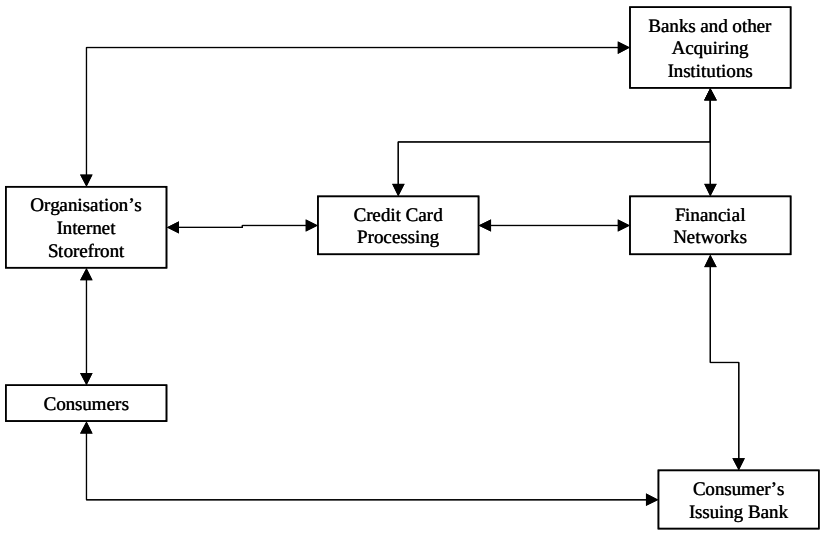


**Figure 2 Transaction Processing Cycle**

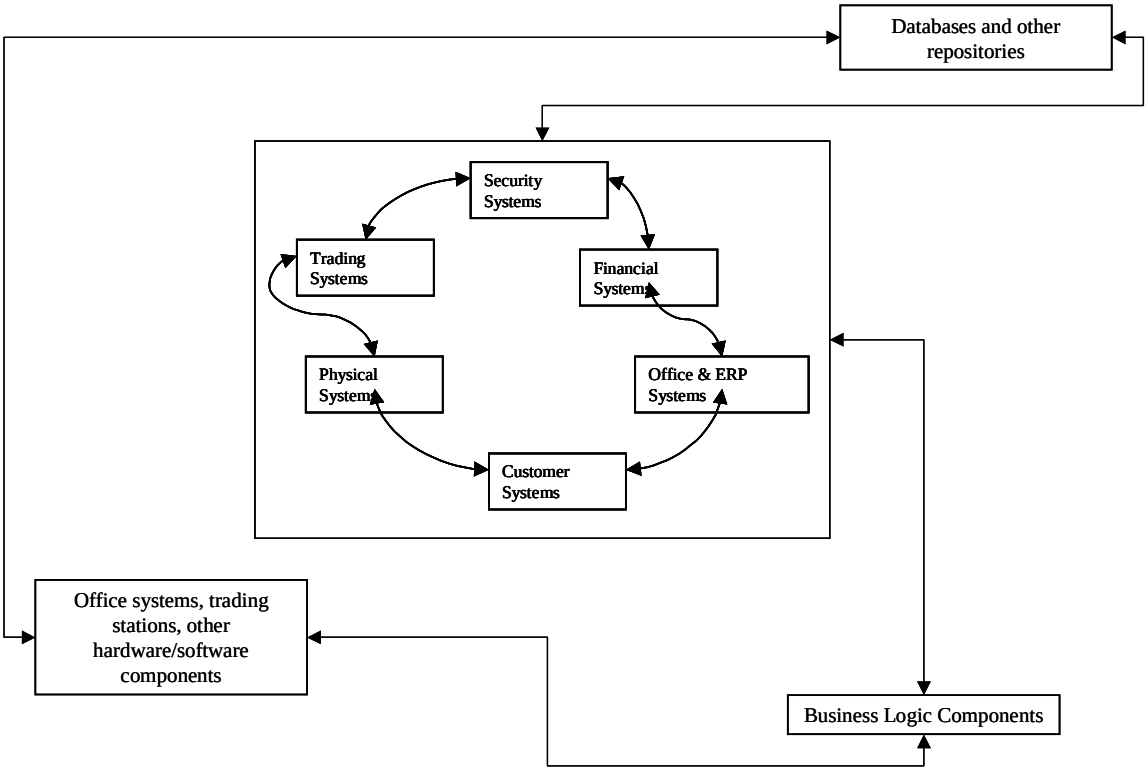


**Figure 3 Business Processing Facilitating Mobile Commerce Transaction**

the consumer's site. The client completes the transaction session by transparently sending a transaction receipt acknowledgment to the server before disconnecting the session.

The whole transaction is accomplished in few seconds, including confirmation back to the customer and the organisation. If the transaction is approved, funds will be transferred to the organisation's account. Once the transaction is confirmed, the transaction will be securely routed and processed. As proof of a securely processed transaction, both the customer and the organisation will receive a transaction confirmation number. This is shown in Figure 2.

The architecture described in this paper supports almost all the elements of the transaction that can be conducted in the organisation. The security aspects not only involve the organisational IT infrastructure but also third-party security levels in order to approve a financial transaction. It should be remembered that consumers expect the organisation to facilitate a reliable and secure transaction and it is in the interests of the organisation that third parties involved in the transaction are reliable and capable of providing the necessary security for the consumer's

transactional details.

While the above diagram (Figure 2) portrays a complete financial transaction system, the subsystem in Figure 3 portrays the component that needs to be supported by an organisation. Components such as office systems, etc., form levels 7-9 in the architecture outlined in this paper. Components such as databases, etc., would form levels 4-6 in the architecture described above. Other components such as Business Logic Components form levels 1-3 in the architecture. The business processing for the facilitation of a transaction is also highlighted.

## 10. Conclusion

The architecture presented in this paper is an attempt to address various new security concerns in the emerging mobile commerce environment. The architecture has been constructed to accommodate various business processes as an integral component and security management system encompassing these business processes. It is believed that this architecture will assist in avoiding issues such as loss of transaction authenticity because the business process is integrated into the security procedures in the architecture. Further, the business processes are kept in the centre of the architecture to enable transaction confidentiality and integrity from an organisational point of view. Further, the interdependence of various systems within the architecture is expected to provide much needed real-time reaction to any cause of transaction unavailability in mobile commerce.

While the architecture is only conceptual, the inclusion of business processes along with IT security is expected to provide tighter controls in terms of financial transactions. This is rapidly becoming essential in the competitive world of mobile commerce where the volume of transactions ensures healthy revenue for organisations. Therefore, the architecture has been conceived with a focus on transaction security. It is hoped that this architecture helps organisations to get a head start in reviewing their security procedures and in establishing a better control on financial transactions.

## References


[1] Anonymous. E-Commerce is growing. *The Australian*, 15 August 2000.

[2] Anonymous. Wireless technology reaches behind the firewall. *Informationweek.com*, June 2000, 30.

[3] Arena, A. Asian Internet start-ups invest heavily in dot.coms. *Australian communications*, February 2000, 15-18.

[4] Craig, J. & Julta, D. *e-Business Readiness: A Customer Focused Framework*. Boston: Addison Wesley, 2001.

[5] Dang, A. V. *E-Business raises transaction security concerns* (Research Note): Gartner Advisory, 2000.

[6] Dang, A. V. *Four action items for E-Business: Transaction Security* (Research Note): Gartner Advisory, 2000.

[7] Deise, M. V., Nowikow, C., King, P., & Wright, A. *Executive's Guide to e-Business: From Tactics to Strategy*. New York: John Wiley & Sons, Inc., 2000.

[8] Dornan, R. *The essential guide to wireless communication applications*. Upper Saddle River, NJ: Prentice Hall PTR, 2001.

[9] Fink, D. Developing trust for Electronic Commerce, in L. Janczewski (Ed.), *Internet and Intranet: Security and Management: Risks and Solutions* (pp. 44-86): Idea Group Publishing, 2000.

[10] Gerrard, M. *Organising for E-Business: Getting it right* (Commentary): Gartner Advisory, 2000.

[11] Ghosh, A. K. *Security and Privacy for E-Business*. New York: Wiley, 2001.

[12] Hayward, S., Dulaney, K., Egan, B., Plummer, D., Deighton, N., & Reynolds, M. *Beyond the Internet: The Supranet* (Commentary): Gartner Advisory, 2000.

[13] Hulme, G. Services Seeks to Bring e-Business to Small Businesses. *Informationweek.com*, August 2000, 21.

[14] Judge, P. Little guys still say NO to the net. *Business Week*, 1998, 134.

[15] Koller, L. Banks flirting with wireless billing. *Bank Technology News*, 2000, *13*, 25.

[16] Langley, N. Get moving on m-commerce. *Computer Weekly*, 11 May 2000, 68.

[17] Lee, A. Small firms must take Internet plunge or risk being sidelined. *The Engineer, 10*, November 2000, 10.

[18] Lewis, T. Ubinet: The ubiquitous Internet will be wireless. *IEEE Computer, 32*, 1999, 10.

[19] Loney, M. M-Commerce safety fears. *IT Week, 3*, 2000, 6.

[20] Schiller, J. *Mobile Communications*. New York: Addison-Wesley, 2000.

[21] Shroeder, S. Wired for business. *Risk Management* March 1999, 12-22.

[22] Smith, D., & Andrews, W. *Exploring Instant Messaging*.: Gartner Research and Advisory Services, 2001.

[23] Stowe, B. Wireless networking looks attractive, but what about the cost of keeping it secure? *Infoworld*, May 2000, 92.

[24] Young, D. Handicapping M-Commerce: Getting ready for wireless e-commerce. *Wireless Review* August 2000, 24-30.

[25] Zhang, Y., & Lee, W. *Intrusion detection in wireless ad-hoc networks.* Paper presented at the ACM/IEEE MobiCom, 2000.